Exhibit B

THE STATE OF WYOMING }
} ss.
CIRCUIT COURT of the }
COUNTY OF NATRONA }

THE STATE OF WYOMING }
Plaintiff, }

Vs. }

760 Landmark Drive #603G }
Casper, Wyoming }
Defendant. }

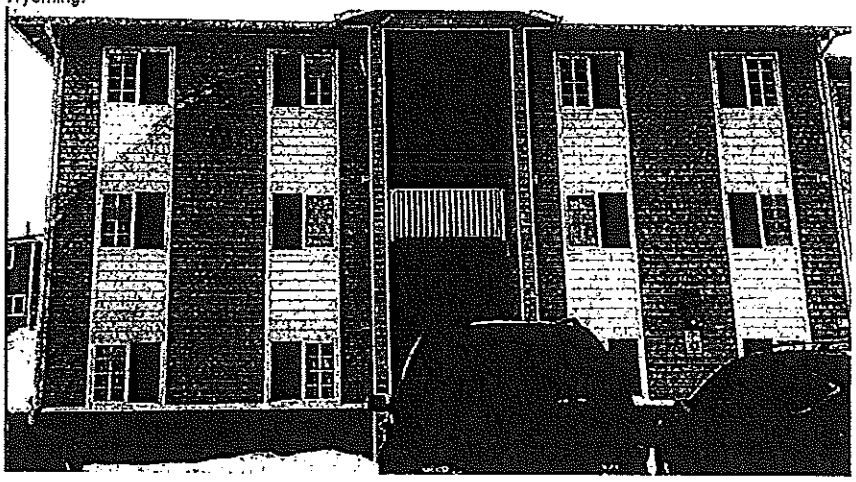
BEFORE: _____
JUDICIAL OFFICER

FILED
FEB 29 2016
CIRCUIT COURT OF SEVENTH JUDICIAL DISTRICT NATRONA COUNTY
BY: _____

AFFIDAVIT FOR SEARCH WARRANT

I, Bruce Dexter, being first duly sworn according to law, on my oath, depose and say:

Within the residence of 760 Landmark Drive, apartment #603G, which is further described as: An apartment, clearly identified by the numerals 603 on its white entry door. The individual apartment is located within a beige and white apartment building, clearly identified by the letter "G" affixed to the outside of the building. The apartment building and apartment are located at 760 Landmark Drive, which is located in the City of Casper, County of Natrona, State of Wyoming:



There is being concealed:

Certain property as described in the "List of Items To Be Seized," annexed and attached hereto as Exhibit "A", and made a part hereof by this reference.

Which is designed or intended for use or which is or has been used as a means of committing a criminal offense in violation of Wyoming Statue 6-4-303.

Is possessed, controlled, or designed or intended for use which is or has been used in violation of any law.

Consists of an item or constitutes evidence which tends to show a crime has been committed, or tends to show that a particular person has committed a crime in violation of Wyoming Statue 6-4-303.

That under provisions of Rule 41 of the Wyoming Rules of Criminal Procedure, a Judicial Officer for the jurisdiction wherein the property sought is located may issue a search warrant to search for and seize any property which constitutes evidence that tends to show a crime was committed and that a particular person committed that crime.

That Affiant requests a search warrant be issued by this court authorizing and directing the warrant officer to search the herein described place to be searched for the above described property, and declares that the grounds for issuance of said warrant are as follows:

EXHIBIT
A

Wyoming DCI
2016-0177
3 of 9

INVESTIGATOR BACKGROUND

a) Special Agent, Bruce Dexter, hereafter referred to as Affiant, is a certified Wyoming Peace Officer employed as a sworn special agent with the Wyoming Division of Criminal Investigation (DCI). Affiant is assigned to DCI Internet Crimes Against Children Task Force (ICAC). Affiant was first certified as a professional peace officer in Wyoming in 1982. Affiant has 39 years of law enforcement experience and spent 20 ½ years with the Laramie County Sheriff's Department before retiring and joining the Division of Criminal Investigation in October of 2006.

b) Affiant has approximately 2900 hours of training recognized and certified by the Wyoming Peace Officers Standards and Training commission and has been trained in the investigation of computer use in the exploitation of children and trained in the methods of forensic analysis of computers used in criminal activity. Your affiant also received training on how various peer-to-peer file-sharing networks operate. Affiant has written or participated in over one hundred search warrants in the State of Wyoming.

c) Affiant has been assigned to operate in an undercover capacity on the Internet by the Director of the DCI for the purpose of identifying and investigating persons attempting to exploit or solicit sexual acts with children.

d) Your affiant has over 200 hours of training related to investigating child exploitation cases and computer forensics.

DEFINITIONS USED IN THIS AFFIDAVIT

e) Internet Protocol (IP) address
An Internet Protocol address is a number that uniquely identifies a computer, or other device that accesses a network, such as the Internet. An IP is used in network communication and is similar in concept to a telephone number.

f) Peer to peer (P2P)
A distributed network architecture, whereby network hosts (computers), can share their resources (such as processing power and storage capacity), or files (such as image and video files) with other hosts without the need for a central managing device.

g) Secure Hash Algorithm (SHA)
SHA1 AND SHA256 are part of a set of cryptographic hash functions designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). Cryptographic hash functions are a kind of algorithm or mathematical operation run on digital data, and by comparing the result (known as the hash) of the algorithm to a known/expected hash value, a person can determine the data's authenticity. An example is running a hash on downloaded software and comparing the result to a published hash of the software. By doing this a user can determine if the downloaded data is genuine. Peer-to-peer file sharing systems use these values to assure the contents of files being shared across the network.

h) Block or Split
A 32KiloByte (kB) block of data that makes up a file. These are referenced to and identified by the SHA256 hash value of the block. When used to identify a block of a file, the hash value is known as the "key" for the block.

i) Node
A computer on the Internet running software that allows it to communicate on a particular peer-to-peer network.

j) Darkweb or Deepweb
Terms to describe networks and Internet use that is not obvious or accessible by the causal user. Most P2P and anonymous networks fall into this category.

OPERATION BACKGROUND

k) Affiant knows through training and experience that the P2P network targeted in this investigation is commonly used to obtain and distribute child pornography. The trading of child pornography on the targeted network occurs on a continual basis and disclosure of the targeted network's actual name would potentially alert users of enforcement action against those using the targeted network to obtain and distribute child pornography. This knowledge would likely encourage users of the targeted network to destroy evidence of illegal activity. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as the "targeted network".

l) Affiant knows the actual name of the targeted network. Affiant also knows through training and experience that because of the way in which the targeted network operates, it is considered to operate on the Darkweb or Deepweb.

m) Your Affiant knows from training and experience that because of the way the targeted network operates, it is adept at keeping a user's activity relatively anonymous. Because of this, the network has attracted persons that wish to collect and/or share child pornography files. The targeted network has not been found to be a significant source of music, adult pornography, theatrical movies or other copyright material

n) Your Affiant knows that the targeted network is an Internet based, peer-to-peer network, which attempts to let users anonymously share files and communicate (chat) on forums. The targeted network utilizes free software and the source code is publicly available.

o) Your Affiant knows that communications between computers running the targeted network software (known as nodes) are encrypted and routed through other targeted network nodes. Because of the method in which computer to computer communication occurs on the targeted network, it is difficult to determine who may be the actual requestor of child pornography files and who is just relaying the request message on behalf of another requesting computer.

p) Your Affiant knows from training and experience that files, or portions of files (known as blocks), are stored on nodes in the targeted network. The files, or portions of files (blocks), are uniquely identified on the targeted network by what is known of as a key. The key is a sequence of alphanumeric characters and uniquely identifies the file, or portion of file, throughout the network. Because of encryption, persons operating computers with stored blocks, are likely to not know the content of blocks being stored on their computers.

q) Your Affiant knows from training and experience that the file portions are distributed across nodes on the targeted network. When a user on the targeted network wants a file, the software is used to create a request message for the different file blocks, identified by their keys. Those request messages are broadcast on the targeted network following the network communication protocol in an attempt to locate a computer on the network that has that particular block stored.

r) Your Affiant knows from training and experience that Internet computers identify each other by an Internet Protocol or IP address. Your Affiant knows that these IP addresses can assist law enforcement in finding the location of a particular computer on the Internet. These IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). Given the date and time the IP address was used, an ISP can typically identify the account holder by name and physical address.

s) Your Affiant knows from training and experience that someone requesting blocks of a file has taken substantial steps to install software to operate on the targeted network and additional steps to locate a file's "key" in order to facilitate a download of that block. The Network provides no search mechanism common to other file sharing systems. A subject desiring to download a file must first find the key(s) associated with the file, such as on a website or message board.

t) In September 2011, law enforcement officers began an undercover operation collecting keys and files being publicly shared on the targeted network, in order to build a data base of keys associated with known or suspected child pornography.

u) In April 2012, law enforcement officers began running copies of software on the targeted network that had been modified for law enforcement to log the IP address, key, and date and time of requests that were sent to these law enforcement nodes. These keys are then compared to keys of known child pornography to identify IP addresses soliciting child pornography.

v) Your Affiant knows that the information collected by the law enforcement version of the software (IP addresses, keys, date and time), is also readily available through use of the public version(s) of the software. The law enforcement version simply makes collection and storage of the information automatic so that it can later be analyzed.

w) Your Affiant knows from training and experience, that multiple requests for blocks of a particular file from a particular IP address can be evaluated to determine if the computer at a particular IP address is the likely requester of the file, as opposed to merely passing on a request originating from another user.

x) Your Affiant knows from training and experience that over fifty search warrants or consent searches have been conducted in the United States and Canada by using the above method of investigation. This method has proven to be reliable in determining the location of computers that were involved in using software on the targeted network to obtain child pornography. By using the above method of investigation, nearly every case was verified through the following means:

1). Evidence of child pornography was found on the computer(s) or other media.

2.) Interviews of persons using those computers verified that child pornography had been present at one time but had been deleted or the computer with the child pornography had been removed from the premises.

3.) Evidence of the use of encryption software to hide files was found on the computer.

CURRENT INVESTIGATION

y) While reviewing requests received by undercover law enforcement nodes. Your Affiant observed IP address 174.45.200.45 routing and/or requesting suspected child pornography file blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file.

z) Your Affiant observed that between 8:41PM UTC on December 26, 2015 and 5:13AM UTC on December 27, 2015 a computer running software on the targeted network, at IP address 174.45.200.45, requested from law enforcement nodes 23,359 parts, or blocks, of the file named "lolita8-famex(momdad2daugh).mpg", (with the SHA1 hash of 607c372e56a4374cd3f660959-ae9da8755ef648a). Your Affiant has previously downloaded the file with the above referenced SHA1 value and knows it to be a video file approximately 59 minutes and 4 seconds in length. It begins with title screen "Tenny-File.LOLITA.8" and depicts a prepubescent female, an early pubescent female, an adult female, and an adult male engaging in various sexual acts. The background features either a bed with a black and white print, or a couch with a circular orange, black, and white print. The movie contains several segments, including, but not limited to: three females, naked, engaging in sexual acts while on a bed; the pubescent female inserting an orange vibrator into the adult's vagina; and the adult female inserting an orange vibrator into the prepubescent child's vagina.

aa) Your Affiant observed that between 6:49PM UTC on December 26, 2015 and 4:19AM UTC on December 27, 2015 a computer running software on the targeted network, at IP address 174.45.200.45, requested from law enforcement nodes 19,639 parts, or blocks, of the file named "A2A (Mom & daughter sex).mpg", (with the SHA1 hash of ee42319fc8a359643fa207da5-8bf85bcef916527). Your Affiant has previously downloaded the file with the above referenced SHA1 value and knows it to be a video file approximately 45 minutes and 29 seconds in length. It begins with a close-up of a female minor, 12-13 years of age. The minor is wearing a dress and takes the dress off. The female minor fondles herself. The video then depicts the minor masturbating a nude adult woman. The video also depicted the female minor performing oral sex on a nude male that appeared to be 12 to 15 years old.

bb) Your Affiant observed that between 10:22PM on December 26, 2015 UTC and 5:55AM on December 27, 2015, a computer running software on the targeted network, at IP address 174.45.200.45, requested from law enforcement nodes, 27584.3 parts, or blocks, of the file named "14Y Girl And Her Little Sis.mpg", (with the SHA1 hash 607c372e56a4374cd3f660959-ae9da8755ef648a). Your Affiant had previously downloaded the file with the above referenced SHA1 hash and knows it to be a video file that is approximately one hour, six minutes and 11 seconds long. There is a caption or title on the bottom of the screen that reads "TI93N". The video begins with two young females. One is wearing glasses and appears to be approximately 11-13 years of age. The second female appears to be younger and approximately 9 - 11 years of age. An adult male comes into view at 03:13 into the video and begins to manipulate the older girl's clothing and rubs her chest. The male then removes the girl's shirt, lays her down and starts masturbating the girl's vagina. The younger girl looks on. The male performs oral sex on the older girl. He then begins using a vibrator on the old girl's breasts and vagina. At 31:24 the older girl performs oral sex on the male. The male performs intercourse with the older female and the video ends with a short clip of the child in a shower.

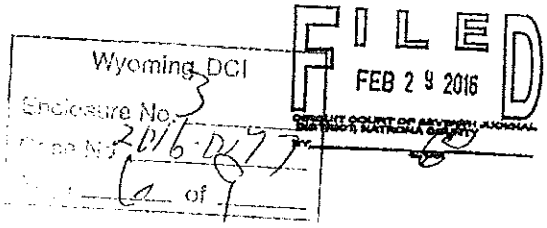
cc) Your affiant conducted a Domain Name System (DNS) check on IP address 174.45.200.45 through the American Registry for Internet Numbers (ARIN). Information from ARIN indicated the IP address was registered to Charter Communications.

dd) Your Affiant spoke with Homeland Security Investigations Special Agent Nicole Bailey, who is assigned to the Wyoming DCI ICAC Task Force and requested that SA Bailey issue an administrative summons (CY-2016-00106R) to Charter Communications to identify the subscriber of IP 174.45.200.45 during the time the IP was seen on *The Network*. The resulting return dated January 27, 2016 included the following subscriber information:

Name:	Bonnie Hebert
Address:	760 Landmark Drive, Unit 603G Casper, Wyoming 82609-4247
IP Information:	IP obtained 11/8/2015 and IP released 12/27/2015

ee) Your Affiant knows that on January 28, 2016 SA Ryan Hleb who is assigned to the DCI office in Casper, Wyoming checked the Casper Police Department for contacts on Bonnie Hebert. Casper Police records indicated Bonnie Hebert lived at 760 Landmark Drive, #603G and that on November 18, 2015 the Casper Police Department had a request for a welfare check on Bonnie Hebert at that address.

ff) Your Affiant knows that on February 4, 2016 Homeland Security Investigations Special Agent Nicole Bailey went to 760 Landmark Drive, Unit 603G and took the photograph that is part of this search warrant and affidavit.



gg) Your Affiant checked the State of Wyoming driver's license files for information on Bonnie Hebert. State of Wyoming records indicated her address was 760 Landmark Drive, 603G, Casper, Wyoming.

COMPUTER EVIDENCE

hh) Affiant knows from training and experience that unlike other kinds of contraband (e.g. drugs), Child Pornography is not consumed by the user. The very nature of computers as a means of collection, transmission, and or storage lends itself to permanent preservation of the actual child pornography or trace evidence that child pornography once resided on he computer.

ii) Affiant knows from training and experience that searches and seizures of evidence from computers may require agents to seize most or all computer items (hardware, software, passwords and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. Computer storage media to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process renders it impractical to attempt this kind of data search on site.

jj) Affiant knows from training and experience that searching computer systems for criminal evidence requires experience in the computer field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

kk) Affiant knows from training and experience that in order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the computer. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as documentation, items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software.

ll) Affiant knows from training and experience that persons trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a persons interest in child pornography or child exploitation.

mm) Affiant knows from training and experience that files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files.

nn) Affiant knows from training and experience that computer software or hardware exists that allows persons to share Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

oo) Affiant knows from training and experience that computers used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the computer as well as ownership and use of Internet service accounts used for the Internet access.

pp) Affiant knows from training and experience that computer crime scenes usually include items or digital information that would tend to establish ownership or use of computers and Internet access equipment and ownership or use of any Internet service accounts to participate in the exchange, receipt, possession, collection or distribution of child pornography.

qq) Affiant knows from training and experience that search warrants of residences involved in computer related criminal activity usually produces items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.

rr) Affiant knows from training and experience that search warrants of residences usually reveal items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

ss) The statements contained in this affidavit are based on this affiant's personal knowledge and information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to this affiant concerning this investigation.

tt) The above information has led Affiant to believe that probable cause exists to believe that the items listed in Exhibit A are evidence of the attempted exploitation of children by means of the possession and/or receipt and/or attempted distribution of child pornography in violation of Wyoming Statute §6-4-303 and are concealed in the residence at 760 Landmark Drive, #603G, Casper, Wyoming.

Further your Affiant sayeth naught.

Bruce Dexter

Subscribed and sworn to before me on the 29th day of February 2016.

Judicial Officer
Circuit Court Judge

FILED
FEB 29 2016
CIRCUIT COURT OF SEVENTH JUDICIAL DISTRICT, NATRONA COUNTY
BY

Wyoming DCI
Enclosure No. 3
Case No. 2016-0177
Page 8 of 9

EXHIBIT A

LIST OF ITEMS TO BE SEIZED

ITEMS TO BE SEIZED

Images or visual depictions representing the possible exploitation of children.

Computers

Cellphones or smartphones

Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.

Computer storage media and the digital content to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography.

Computer software and application software installation and operation media.

Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

If computers are found in a running state the investigator may acquire evidence from the computers prior to shutting the computers off. This acquisition may take several hours depending on the volume of data.

Manuals and other documents (whether digital or written) that describe operation of items or software seized.

Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, collection, origin, manufacture or distribution of images involving the exploitation of children.

Correspondence or other documents (whether digital or written) exhibiting an interest in the exploitation of children.

Items or digital information that would tend to establish ownership or use of computers and Internet access equipment and ownership or use of any Internet service accounts to participate in the exchange, receipt, possession, collection or distribution of child pornography.

Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements, U.S. birth certificate, U.S. passport, consular report of birth abroad, certificate of citizenship, certificate of naturalization, permanent resident card, employment authorization document, foreign passport, doctor's bills, subscription bills, social security card, W-2 form, bank statement, any official or government document, rent receipt, mortgage document, vehicle registration, pay stub, tax document, voter registration, report card, magazine bill, doctor's bill and other identification documents

At the discretion of peace officers serving the warrant, photographs and videotaped images may be obtained of the place to be searched for comparison with images and video recovered relating to the investigation of the exploitation of children.

State of Wyoming
Division of Criminal Investigation
Receipt

ITEM #	DESCRIPTION	QUANTITY
100	Black Antec Desktop Computer - Generic	1
101	Blue/Silver Departure Energy Services USB	1
102	Black/Silver Natrona County Schools USB	1
103	PNY 64 GB SD Card	1
104	Lenovo Laptop Computer w/PS SN: L3-Q3015 0804	1
105	LG G Pad Tablet SN: 504CQSF246814	1
106	PNY 4GB SD Card from Nikon Camera	1
107	SanDisk Cruzer 1GB SN BB0805RCIB	1
108	USB Thumbdrive with no cover	1
109	Silver Cruzer Micro 1GB	1
110	Kingston USB White/Red Thumbdrive	1
111	Pebble 301BL Watch SN 15241 4E026U	1
112	Samsung AT&T Cell Phone SGH-I547 SN: R38F400YARR	1
~~113~~	~~Summer Infant SN: 12120304 White/Silver~~	~~1~~
114	Alienware Laptop Svc Tag: BDCCLVIM14X-RZ	1
115	Tosiba 2TB Ext HDD SN: 5F08SB1W	1
200	Nikon Camera SN: 32602114 + 4GB PNY	1
116	Black Antec Desktop Computer - Generic w/sticker on side "TUF INSIDE THE ULTIMATE FORCE"	1
117	White Kingston USB Thumbdrive w/purple loop end	1

END

Received From: Kyle Hebert - Casper WY (for)
Received By: Mark Timmons WY/Dave Lester WY

Wyoming DCI
Enclosure No. 4
Case No. 2016-0177
Page 1 of 1

Date: ~~Feb 29 2016~~

Page # 1 of 1

CASE # 2016-00177

100 - Living Room/Desk Area
200 - Master Bedroom

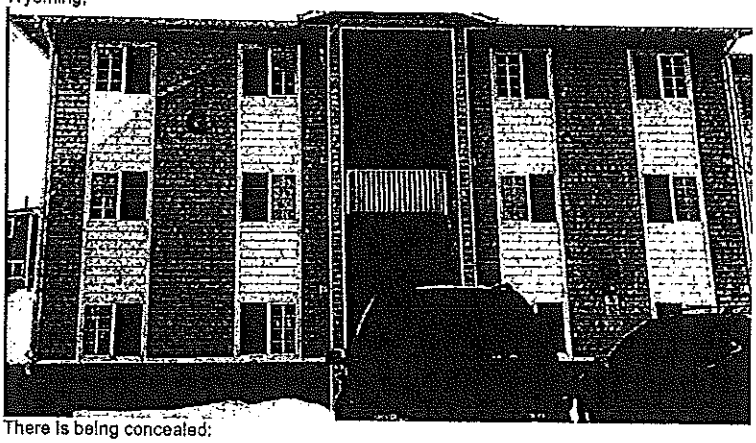
THE STATE OF WYOMING)
)
CIRCUIT COURT of the) ss.
COUNTY OF NATRONA)
)
THE STATE OF WYOMING)
Plaintiff,)
)
Vs.)
)
760 Landmark Drive #603G)
Casper, Wyoming)
Defendant.)

BEFORE: _____
JUDICIAL OFFICER

FILED
FEB 29 2016
CIRCUIT COURT OF SEVENTH JUDICIAL DISTRICT NATRONA COUNTY, WY
BY: _____

SEARCH WARRANT

To: DCI Special Agents and other law enforcement personnel.
Affidavit having been made before me by Bruce Dexter that he has reason to believe that:
Within the residence of 760 Landmark Drive, apartment #603G, which is further described as: An apartment, clearly identified by the numerals 603 on its white entry door. The individual apartment is located within a beige and white apartment building, clearly identified by the letter "G" affixed to the outside of the building. The apartment building and apartment are located at 760 Landmark Drive, which is located in the City of Casper, County of Natrona, State of Wyoming;



There is being concealed:

Certain property as described in the "List of Items To Be Seized," annexed and attached hereto as Exhibit "A", and made a part hereof by this reference;

Which is designed or intended for use or which is or has been used as a means of committing a criminal offense in violation of Wyoming Statue 6-4-303;

Or which is possessed, controlled, or designed or intended for use or which is or has been used in violation of any law;

Or consists of an item or constitutes evidence which tends to show a crime has been committed, or tends to show that a particular person has committed a crime in violation of Wyoming Statue 6-4-303;

And as I am satisfied that probable cause has been shown to believe that grounds exist for the issuance of the Search Warrant, said probable cause for said grounds being contained in the Affidavit of Bruce Dexter annexed and attached hereto as Exhibit "B", and made a part hereof by this reference;

You are commanded to search the above described premises, vehicles and buildings for the property specified, serving this warrant and making the search between the hours of 6:00 a.m. and 10:00 p.m., and within ten (10) days, and if the property be found there, to seize it, prepare a written inventory of the property seized, and bring the inventory before me.

Dated this 29th day of February 2016.

Judicial Officer
Circuit Court Judge

Wyoming DCI
Enclosure No. 3
Case No. 2016-0173
Page 1 of 9

EXHIBIT A

LIST OF ITEMS TO BE SEIZED

ITEMS TO BE SEIZED

Images or visual depictions representing the possible exploitation of children.

Computers

Cellphones or smartphones

Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.

Computer storage media and the digital content to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography.

Computer software and application software installation and operation media.

Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

If computers are found in a running state the investigator may acquire evidence from the computers prior to shutting the computers off. This acquisition may take several hours depending on the volume of data.

Manuals and other documents (whether digital or written) that describe operation of items or software seized.

Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, collection, origin, manufacture or distribution of images involving the exploitation of children.

Correspondence or other documents (whether digital or written) exhibiting an interest in the exploitation of children.

Items or digital information that would tend to establish ownership or use of computers and Internet access equipment and ownership or use of any Internet service accounts to participate in the exchange, receipt, possession, collection or distribution of child pornography.

Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements, U.S. birth certificate, U.S. passport, consular report of birth abroad, certificate of citizenship, certificate of naturalization, permanent resident card, employment authorization document, foreign passport, doctor's bills, subscription bills, social security card, W-2 form, bank statement, any official or government document, rent receipt, mortgage document, vehicle registration, pay stub, tax document, voter registration, report card, magazine bill, doctor's bill and other identification documents

At the discretion of peace officers serving the warrant, photographs and videotaped images may be obtained of the place to be searched for comparison with images and video recovered relating to the investigation of the exploitation of children.